WHAT IS CLAIMED IS:

1. In a computing environment having a connection to a network, computer readable code readable by a computer system in said environment, for enabling a server computer within the computing environment to both authenticate a user of a client computer within the computing environment and to verify that the user is authorized to request that the server computer carry out a requested action, comprising:

a digital certificate assigned to the user of the client computer, the digital certificate comprising a first code portion and a second code portion,

wherein the first code portion of the digital certificate is configured enable authentication of the user, the first code portion defines a public key, a certificate serial number, a certificate validity period, a digital signature of the certificate authority, and an extension field,

and wherein the second code portion of the digital certificate is configured to define an authority of the user of the client computer to request that the server computer carry out the requested action, the second code portion being configured for inclusion within the extension field of the first code portion, the authority of the user defined within the second code portion of the certificate being verifiable by the server computer independently of the digital certificate.

2. The computer readable code of claim 1, wherein the digital certificate conforms to the X.509 standard.

3. The computer readable code of claim 1, wherein the second code portion is configured as XML code.

4. The computer readable code of claim 3, wherein the XML code is compliant with a DSML standard.

5. The computer readable code of claim 1, wherein the authority of the user of the client computer is stored in a hierarchical authority data structure that is accessible by the server computer.

6. The computer readable code of claim 1, wherein the authority of the user defined within the second code portion of the certificate is verifiable by the server computer accessing a store of authority information that is independent of the received certificate.

7. The computer readable code of claim 1, wherein the authority defined within the second code portion defines access rights of the user to data and programs within the computing environment.

8. The computer readable code of claim 1, wherein the authority defined within the second code portion defines rights of the user to issue payment requests.

9. A computer-implemented method for ensuring non-repudiation of a payment request, the payment request being generated in a computing environment having a connection to a network, the method comprising the steps of:

receiving, over the network, the payment request together with a certificate identifying a user having caused the payment request to be generated, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information defining an authority of the user to make the payment request;

validating the certificate-identifying information and the user-identifying information included within the received certificate;

validating the authority information included within the received certificate, and

executing of the payment request only when the certificate-identifying information, the user-identifying information and the authority information within the received certificate is successfully validated.

10. The method of claim 9, wherein the payment request is for a predetermined amount and wherein the payment request is authorized only when the validating steps are successful and when the authority information for the user stored in the hierarchical authority data structure lists an authorized amount for the user at least equal to the predetermined amount.

11. The method of claim 9, wherein the certificate received in the receiving step conforms to the X.509 standard.

12. The method of claim 9, wherein the authority information is configured as XML code.

13. The method of claim 9, wherein the XML code is compliant with a DSML standard.

14. The method of claim 9, wherein the authority information is validated by accessing a store of authority information that is independent of the received certificate.

15. A software application configured to carry out a financial transaction, the application being configured to run on a computer coupled to a network, and comprising, stored on a computer-readable medium:

certificate receiving code which is configured to receive a digital certificate from a user over the network, the certificate including certificate-identifying information and user-identifying information, the certificate further including authority information that defines an authority granted to the user to request that the financial transaction be carried out;

certificate validating code configured to enable validation of the certificate-identifying information and user-identifying information within the received certificate, and

authorization validating code configured to enable validation of the authority information within the received certificate against corresponding authority information for the user stored in a data structure that is independent of the received certificate.

16. The software application of claim 15, wherein the digital certificate conforms to the X.509 standard.

17. The software application of claim 15, wherein the authority information is configured as XML code.

18. The software application of claim 17, wherein the XML code is compliant with a DSML standard.

19. The software application of claim 15, wherein the authority defined by the authority information within the received certificate also defines rights of the user to access predetermined data and programs within the network.

20. A computer-implemented method for controlling authority of employees of a company within in a computing environment, the company having a hierarchical management structure, the method comprising the steps of:

creating or receiving a primary digital certificate, the primary digital certificate including primary authority information that defines and grants primary rights to a primary employee as defined by the hierarchical management structure;

creating secondary digital certificates and assigning the created secondary certificates to selected secondary employees requiring access to the computing environment, each of the selected secondary employees occupying a predefined position within the hierarchical management structure that is hierarchically lower than that of the primary employee, each of the secondary certificates including secondary authority information that defines and grants secondary rights, the secondary rights being derivative from the primary rights and being commensurate with the predefined position of the selected secondary employee within the hierarchical management structure, and

allowing each selected secondary employee to exercise only those rights within the computing environment that are granted by the secondary rights defined within the assigned secondary certificate.

21. The computer-implemented method of claim 20, wherein the primary and secondary certificates conform to the X.509 standard.

22. The computer-implemented method of claim 20, wherein the primary and secondary authority information are encoded within the primary and secondary certificates as XML code.

23. The computer-implemented method of claim 22, wherein the XML code is compliant with a DSML standard.

24. The computer-implemented method of claim 20, wherein the secondary rights defined within at least one of the secondary certificates are derivative from secondary rights defined within another secondary certificate.

25. The computer-implemented method of claim 20, further including a step of revoking a secondary certificate to a terminated secondary employee, the revoking step being operative to revoke all certificates to secondary employees of the company that report to the terminated secondary employee, which revokes all secondary rights that are derivative from the secondary rights granted by the revoked secondary certificate.

26. The computer-implemented method of claim 20, further including a step of revoking a secondary certificate to a terminated secondary employee, the revoking step being operative to revoke all secondary rights that are derivative from the secondary rights granted by the revoked secondary certificate.

27. The computer-implemented method of claim 20, wherein the primary and secondary rights define access rights to data and programs within the computing environment.

28. The computer-implemented method of claim 20, wherein the primary and secondary rights each define amounts to which the primary and each of the secondary employees, respectively, are authorized to bind the company.